Testimony before the U.S. – China Economic and Security Review Commission
Hearing on "Chinese Investment in the United States: Impacts and Issues for Policy Makers"

Jeffrey Z. Johnson
President & CEO, SquirrelWerkz
January 26, 2017

Thank you for the opportunity to testify before the esteemed members of this commission. The works and research associated with this commission have long served as a valuable resource to those of us in the cyber, competitive and economic threat intelligence and risk management profession. Through today's testimony I plan to present new insights into the Chinese affiliated cyber-economic (CE) campaigns and how the government of China leverages a number of direct and indirect entities and methods to illegally finance, and/or subsidize, these complex industry-wide efforts.

Before I begin the formal portion of my testimony, I would like to state that I assess our biggest challenge to be identical to that described by the 9/11 Commission when they described the root cause of the intelligence failure related to the terrorist attacks on our nation's economic and military epicenters in 2001. They stated that our nation experienced a ***"failure of imagination, policy, capabilities and management."*** In a similar regard, despite the volumes of evidence and damage assessments presented annually about the nature and impact of the Chinese threat to our economic and national security, we attempt to rationalize and forgive our adversary's actions and behaviors because we tend to "hope" we'll ultimately change China into a market-driven economy and a nation accepting of fair trade, transparency and the rule-of-law as we know it.

From a background perspective, I've had the privilege of leading two teams over the past four years in the development, refinement and automation of what's referred to as cyber, competitive and economic threat intelligence. This is a form of predictive intelligence used to expose the breadth, depth, activities, entities and objectives associated with nation-state affiliated cyber-economic campaigns. These campaigns consist of state-sponsored and supported criminal cartels focused on leveraging cyber-enabled espionage and sabotage to execute industry-wide fraud, market manipulation and anti-trust schemes designed to accelerate China's entry and domination of each key global industry. In effect, these campaigns are designed to selectively bypass traditional barriers-to-entry that would otherwise prevent weaker competitors from earning a market leadership position within a free-market – especially within the more complex technical and scientific markets.

These cyber-economic campaigns are persistent, intense, patiently executed and include the simultaneous execution of such a large and diverse set of legal and illegal methods, individuals and organizations, there's little chance the targeted U.S. competitors can effectively defend or compete in the future without significant support of the U.S. government. If we begin with a mutual appreciation of this basic premise, we will be able to better understand how China's so-called private investment strategy, and related CE activities, fit within the broader context of China's strategic economic and military plans and activities while also addressing the one-sided, "in-the-trenches," battles being fought every day and how to begin turning back the tide.

Nearly every issue we will discuss today is a practice forbidden by US law and the WTO – an enforceable agreement China entered into in 2001. The sections of the WTO agreement pertaining to these issues include: 1) Annex 1, Section 17, **Barriers-to-Entry**, 2) Annex 1, Section 19, **Anti-Dumping** and 3) Annex 1, Section 24, **Subsidies and Countervailing Measures**. Rather than addressing the practices giving rise to these allegations, China has aggressively pressured governments for recognition as a market economy, a move which would limit the severity of the penalties implemented on China through the WTO's dispute settlement mechanism.

If we are to stop the type of behavior described throughout my testimony and protect our economic and national security, these laws and/or agreements must be applied to the fullest extent of the law and we must proactively manage the proper defense, enforcement and punitive efforts in a unified, centrally controlled, manner. And, we must do so in a manner that is consistent with what's required to counter our adversary's significantly superior cyber-economic capabilities. The U.S. may be superior in the execution of traditional business, commerce, financial, production, education, innovation, enforcement, military defense and intelligence processes. But, in the case of cyber-economic conflicts, our strengths are our greatest weaknesses because each is treated as a separate and distinct function and our laws and organizational structures prevent us from identifying and acting upon nation-state threat actor's intent on exploiting these weaknesses through the execution of a centrally controlled national strategy designed to achieve economic, military and diplomatic superiority. Chinese leaders refer to this as "Unrestricted Warfare."

Our own laws and corporate risk statements become the starting point for their targeting plans. For example, one need only Google the terms fraud, market manipulation and anti-trust to view a host of laws, regulations, reports, guidelines and case studies that describe, in detail, how to execute schemes associated with each category of crime and how to legally defend oneself if detected. Then, download just one corporate annual report from each industry and review the "Risk Factors" section. Any current or former "Targeting" or "Mission Planning" analyst will confirm just how valuable this information would be to a cyber-economic campaign planning professional – especially if the adversary believes the targeted nation(s) or corporation(s) are unable to detect, and unwilling to act upon, the national level aspects of the crimes.

But, we need not change who we are nor implement policies that result in less transparency or unintentional trade/currency wars. Nor should we open ourselves to charges of engaging in our own form of protectionism. Our focus simply needs to be improving upon our strengths while also improving our ability to expose and act upon nation-state adversary weaknesses and their illegal activities. We place our focus on improving fair and open competition and put Chinese owned, controlled and highly infiltrated companies on notice that we know what they have done, how they've done it and we will not tolerate it in the future. We place the emphasis on the beneficiary entities the same way we would if we discovered a U.S. company or investor was involved in fraud, market manipulation and anti-trust schemes. And, we also hold all entities materially contributing to these efforts equally accountable. We can simply refer to it as maximizing our ability to compete, as a nation, in the 21st century.

I would also like to say, for the record, that my testimony is my own personal opinion based on my direct experiences over the past 35 years within the intelligence, information warfare, information

security, fraud control and financial services communities. All examples and evidence presented are provided for information purposes only and the commission, and public, are encouraged to review the same and come to their conclusions as to the validity of my findings and recommendations.

What are the Main drivers of Chinese investment in the United States?

The underlying political, economic and military drivers associated with China's cyber-economic campaigns, and the associated financing methods, appear to be heavily driven by fear – and justified fear at that. Following the Chinese Cultural Revolution and Chairman Mao's death, the Communist Party Elite reportedly felt a desperate need to catch up to the West as they realized that they were falling further and further behind in technological and economic strength and this placed the Communist Party, and its leadership, at risk. This feeling of desperation to improve its education, infrastructure, technological and economic leadership position appears to have escalated to new heights after China's Communist Party leadership studied the 1990-1991 U.S. Gulf War (Desert Storm). Reports indicate many of China's most senior leaders were stunned when the U.S. technological superiority resulted in the near destruction of the world's 6th largest army in just 100 hours - with only 147 coalition forces killed-in-action compared to 20,000 to 35,000 Iraqis. In addition, the Iraqis lost approximately 3,700 tanks, 2,400 APCs, 2,600 artillery pieces, 110 aircraft and 19 naval ships. This, along with growing internal issues associated with sustaining and controlling a poverty stricken population of approximately 1.3B people and the seemingly insurmountable challenges of overcoming the miserable state of its public and private infrastructure, potable water, agriculture, livestock, medical and healthcare, education and the effects of the "one child" policy, created the drivers and justification for the ongoing cyber-economic campaigns and the corresponding surge in Chinese Outbound Foreign Direct Investment (FDI).

The more traditional and obvious objectives associated with China's cyber-economic campaigns are:

1. Protection and strengthening of the communist party
2. Job creation
3. Economic and workforce development
4. Gaining increased levels of diplomatic influence

But, China's objectives also extend well beyond western norms, and in many cases, our imagination. Chinese outbound FDI is but one piece of a much bigger, and more complex, strategic mosaic. This bigger puzzle is, to quote a former White House official, "a Pandora's Box." It has been intentionally designed as a Pandora's Box to discourage us all from fixing it. You may recall that the real Pandora's Box was actually a jar containing all the evils of the world and Pandora let everything out except for "hope." Our adversary would like to create the same conditions – conditions of hopelessness. Only then will their enemy submit "without firing a shot."

The more aggressive and unique objectives of these campaigns and investment activities include:

1. Gaining monopoly-like control of key industries and the global economy.
2. Gaining increased control of each company's value and supply-chain.
3. Materially infiltrating key financial, corporate, research and government entities.

4. Gaining enhanced insider access to sensitive IP and technology otherwise off-limits or beyond their current capability
5. Gaining increased dependence on Chinese financial resources for financial and economic growth.
6. Gaining control of the western investment syndicates in order to redirect their O-FDI toward China's preferred investments.
7. Decreasing risk associated with the exposure of their illicit financing operations.
8. Increasing control of domestic and overseas Chinese individuals (hereditary – not just current Chinese citizens).
9. Increasing levels of political influence and control within the U.S. and other nations.

Do Chinese investments and activities present economic or business challenges for the United States? Foreign investment in to U.S. entities by the Government of China and its proxies is our 21st Century Opium and, if not managed and controlled, it will likely lead to the eventual loss of our strategic competitive advantage in banking, finance, innovation and productivity. China's investments are made within the context of the aforementioned cyber-economic campaigns – not traditional Return-on-Investment (ROI) principles. Based on my experience with the various industry cyber-economic campaigns, I believe China's primary investment related objectives fit within the following categories:

1. Concealment of illegal government subsidies in support of building national champions or top tier, controlled, competitors
2. Concealment of government financing of covert, U.S. based, Chinese controlled entities serving in various cyber-economic campaign support roles such as:
    - Technology transfer
    - Espionage support
    - Sabotage support
    - Support the insertion, through mergers, of Chinese teams or business units within strategic U.S. companies for the purposes of technology transfer, espionage and sabotage
    - Capacity building
3. Concealment of government investments in companies to:
    - Enhance private equity syndicates and raise capital for strategic Chinese investments
    - Gain access to sensitive insider information (sales, performance, risk, legal, investment, etc.)
    - Manipulate foreign industry leaders
    - Gain access to sensitive technology and related IP
    - Support corruption (bribes and money laundering)

The following summarizes the national and economic issues/challenges associated with these efforts:

1. <u>Concealment of illegal government subsidies in support of building national champions or top tier, controlled, competitors:</u> When an illegitimate Chinese investor (private equity or corporations) provide financing to an illegitimate Asset/Company (i.e., unqualified and state supported entity) they artificially increase the competitiveness (price and options) and market share of an entity that would otherwise be considered a non-performing asset. Conversely, this weakens the legitimate competitors and reduces their market share, cash and liquidity position, growth capital and ultimately results in: a) insolvency, b) being acquired by the Chinese champions or c) being acquired

by other weakened survivors. In each case, removal of the legitimate competitors and the free-market dynamic will typically prevent the recovery of the former market leaders and ultimately discourage investor participation in the stock market thus placing the de facto state-owned-enterprises in permanent monopoly positions.

2. Concealment of government financing, and control, of covert, U.S. based, Chinese entities serving in various cyber-economic campaign roles: This method is typically used in support of corruption, money-laundering, concealment, deception and to develop corporate or other forms of CE Campaign support entities that can more easily, including as trusted insiders, interact with U.S. based entities, investors and customers. This approach allows China controlled business and investor entities to gain highly trusted insider access to companies that compete with the Chinese national champions as well as their customers and other value-chain entities. This provides an enormous competitive advantage to the entire Chinese affiliated corporate and investor cartel.

3. Concealment of government investments in companies: This method includes outbound investments from Chinese entities with the intent of: a) creating strong personal relationships with U.S. investors, b) increasing China's overall industry influence and access, c) buying privileged access to private/confidential corporate decision making information with intent of sharing with China competitors or for use within cyber-economic schemes, c) gaining control of the U.S. asset and its products and IP for use within cyber-economic schemes, and d) gaining control of the U.S. asset to gain access to critical supply and/or value chain entities. Evidence suggest this method is also used to generate revenue/capital required to "self-fund" some level of the cyber-economic campaigns. Methods used to entice or force a target company to accept the terms of the Chinese investor include coercion and duress.

How can these challenges be mitigated?

This is not an insurmountable problem and it is one we have much more control of than China would like us to believe – at least as of 2017. They prefer we accept the hopelessness of defense and just enjoy the opium of foreign investment – a narcotic ultimately to be withheld when the house-of-cards collapses or they've achieved their stated objectives. The U.S. is still the strongest nation in the world in terms of innovation, consumer strength, education and a motivated workforce – and despite losing 77 spots on the Fortune 500 between 2002 and 2015, the U.S. is still the leader with 128 companies listed. Unfortunately, China grew from 3 to 106 during the same period.

I believe the solution to these cyber-economic campaigns is based upon two primary principles: 1) Enhancing current laws and regulations to address nation-state cyber-economic threats vs. drafting new laws and regulations and 2) Enhancing our government/industry command and control structure to address ***cyber-enabled economic warfare***.

As for the more detailed recommendations, I believe that if the following were formalized and acted upon, we would see a remarkable reversal of the current campaigns while at the same time balancing the need to cure the disease without killing the body. In this case, China is a major part of the global economy, the body, and any step taken to correct the cyber-economic related issues must correct the

issue without causing the complete collapse of China's economy or government. Therefore, I recommend the following:

1. Optimize government and industry awareness of the current state of each nation-state cyber-economic campaign (by industry)
2. Optimize government and industry awareness of the CE campaign strategies, methods, activity, communications and coordination
3. Empower a joint cyber-economic task force to act upon nation-state cyber-economic campaign activity within the context of a strategic national threat
4. Enhance audit, due diligence and procurement practices and standards to include cyber, competitive and economic threat intelligence methods and techniques
5. Eliminate current audit community conflicts-of-interest introduced by rogue nation-state involvement in cyber-economic campaigns (i.e., rogue nation-state introduced obstructions to growth and regulatory retaliation in response to adverse findings)
6. Create a model CE procurement risk management program using the FAR/DFARS procurement processes
7. Create a model CE investment portfolio risk management program using the top U.S. government pension programs (e.g., Civil Service Retirement and Disability Fund, Thrift Savings Plan, Military Retirement Fund, Congressional Pension Fund)
8. Create a model CE insider threat management program by focusing on the Defense Industrial Base and Defense Security Services (DSS)
9. Optimize the U.S. immigration and visa programs to reduce the number of high-to-severe risk insiders supporting CE espionage, sabotage and support related activities
10. Identify and revoke the visa's associated with the Top 5-10 U.S. based CE threat entities per industry campaign
11. Leverage existing US, China and Taiwanese laws to jointly pursue prosecution of the top 100 CE threat actors (people) within China, Taiwan and the U.S. involved in the most material campaign schemes over the past 5-10 years.

If these measures do not result in a significant shift away from the use of cyber-economic campaign methods, then include:

1. Place the highest risk and confidence Chinese industry, academic and government CE leadership entities (threats, accomplices and beneficiaries) on the official U.S. OFAC and travel restrictions lists
2. Pursue trade sanctions and significant civil awards in support of the CE victim companies, shareholders, universities and research organizations

Can you explain the private equity, private corporation and SOE investor roles and activities within the context of what you believe are the most significant Chinese government affiliated industry campaigns?

<u>Priority #1 – IT Industry Overview:</u>

I've divided the IT Industry Campaign into seven sub-campaigns: 1) Raw Materials, 2) Component Makers, 3) Telecom/Wireless Service Provider, 4) Network & Communications, 5) End-User Platform and Mobile, 6) IT Security and 7) Digital Content.

The net result of this campaign is that Huawei, ZTE, Lenovo, Tsinghua Holdings, Xiaomi, Netscreen, Fortinet, NSFocus and Hillstone Networks appear to be the primary beneficiaries of the earliest phases of this campaign. Conversely, Nortel, Alcatel, Lucent, 3Com, RIM/Blackberry and Motorola have been sidelined while Ericsson, Cisco, Nokia, Juniper and IBM have been degraded but remain on the leader board.

Each segment continues to be targeted but the more intense current cyber-economic activity appears to be associated with: 1) completing control of the mobile device segment, 2) expanding control of the information technology segment, 3) achieving control of the IOT related segments, 3) leveraging Chinese and Taiwanese resources and assets to execute the microchip campaign and 4) expanding and merging the media and entertainment campaign to control the gaming, content and digital delivery technology segments.

<u>Huawei/ZTE Only CE Campaign Highlights (2005-2014):</u>

Financial Impact

1.	Estimated total victim company lost/diverted revenue:	$160B
2.	Estimated total victim company lost/diverted profit:	$8B
3.	Estimated total government tax (payroll and corporate) income lost:	$19B
4.	Estimated total victim company lost/diverted CAPX and R&D investment:	$11B

The Telecom/Wireless, Network & Communications and End-User Platform/Mobile cyber-economic campaigns were primarily led by Huawei/ZTE but were joined by other government subsidized mobile competitors in the 2011-2013 timeframe. This particular campaign is considered a generation one China-based brute-force CE campaign. The new campaigns are significantly more refined.

During the 10-year period from 2005 to 2014, the top 3 western Telecom/Wireless and Network/Communications competitors grew an average of 4% per year while Huawei/ZTE averaged 24% per year. During this period, Huawei/ZTE developed competitive products that fit within four separate, highly competitive and costly, segments: 1) Telecom/Wireless, 2) Network & Communications, 3) End-User Platform and Mobile and 4) Integrated Circuits. The Western leaders associated with each segment were Ericsson, Cisco, Samsung (RIM/Blackberry for a time) and Intel. Each of these market leading companies invested an average of $6B per year in R&D during the 2005 to 2014 timeframe to earn the leadership position, develop a market leading product portfolio, generate the necessary patents to protect their return-on-investment and optimize growth. This represents an estimated 10 total of $240B invested in R&D by the top competitors associated with these four segments. If a new market entrant were to enter the market and attempt to compete with each, it would be expected to invest an equal, or higher, amount to catch up and overcome each of the leaders.

During the 2005-2014 period, Huawei and ZTE invested approximately $40B. This represents an investment gap of at least $200B within the R&D category alone. This gap also represents the likely value of the illegal R&D subsidies provided by the Chinese Government. Evidence suggest, the $200B value is divided between: 1) illegal cash subsidies to the beneficiary company R&D efforts, 2) illegal cash subsidies to accomplice companies, research institutes, tech transfer organizations, and universities that funnel their IP to the beneficiary, 3) investments in corporate espionage programs and 4) the acquisition of technology and IP.

Despite this disparity, Huawei/ZTE closely mirrored three of the segment leader's product launch rate while exceeding their patents filed rates. The only segment with a material lag in development has been within the microchip segment but this began to accelerate over the past few years. Huawei and ZTE, combined, currently rank #1 in total patents filed in the world. As individual companies, ZTE ranks #2 and Huawei ranks #3. Only IBM filed more patents during this period.

During this same 2005-2014 timeframe, the four western leaders invested an estimated total of $32B in CAPX (facilities, manufacturing lines, IT etc.) required to support growth and annual enhancements to productivity and quality. Huawei/ZTE invested an estimated total of $6.5B. This represents an investment gap of at least $25.5B. As with the R&D investment gap, this shortfall represents the likely value of the illegal CAPX subsidies provided by the Chinese Government.

The likely R&D and CAPX subsidy value of $225.5B over 10 years, or an average of $22.55B per year, is staggering and truly highlights the true magnitude of the issue.

Intelligence information and artifacts analyzed during the analysis and reporting portion of the Huawei/ZTE campaign, included indicators of cyber and traditional forms of espionage, IP theft and conversion, sales manipulation, major levels of concealed subsidies, collusion, exclusive dealing, tying products, predatory pricing, financial statement fraud, coercion, dumping, bid rigging, stock bashing and the introduction of barriers-to-trade. The evidence relates to events within China, Canada, U.S. Africa, Latin America, Caribbean and Southeast Asia.

Information Security Segment Campaign Highlights (1995-2016):

The IT Security Campaign is a very different form of cyber-economic campaign. Same objectives and progress but this campaign likely included significant U.S. based Chinese command and control, corporate, investor and insider threat entities.

The campaign began in the 1995-2000 timeframe. The individuals associated with likely leadership roles entered the U.S. during the late 1980's and early 1990's. They were ***children of the Chinese Cultural Revolution*** and their parents and teachers were children of WWII, the Communist Revolution and the Great Leap Forward.

In 1975, Deng Xiaoping wrote Mao Zedong and stated "University Graduates were not even capable of reading a book in their own fields when they left the university." In addition, in 1993, only 10% of Chinese had a phone, only 1% had a computer at home and their first permanent internet connection

was completed in 1994. Compared to the U.S., approximately 93% had a phone, 50% had a computer, 50% had access to the internet and 30% had a cellphone. This is important context for understanding the leaders and strategic insiders associated with the cyber-economic campaigns.

Three of the four suspected leaders of the IT Security Campaign attended Tsinghua University during the 1981-1989 timeframe. The fourth attended Tsinghua University between 1987-1994. The academic quality associated with this timeframe was far from western standards and each would have likely arrived in the U.S. at a considerable disadvantage in terms of educational building blocks and experience within the subjects of business, finance, management and internet related technologies and security – and even more so in regards to microchips and internet-based encryption.

The suspected leaders of the IT Security Campaign took slightly different paths to NetScreen once they arrived in the U.S. During the years leading up to the 1997 founding of NetScreen, one founder took a position with Intel (Microchips) while another worked at Cisco (an IT network and security pioneer). The initial NetScreen prototype solution used to gain initial funding was allegedly designed and built within a 30-day period while the two individuals continued to work at Cisco and Intel. The original investors included U.S. and Taiwanese venture financing yet traditional due-diligence models would have likely flagged such an investment as a high risk venture.

Campaign Highlights are as follows:

1998: NetScreen leadership co-found Hua Yuan Science and Technology Association (HYSTA) – the suspected primary U.S. based IT Industry cyber-economic command and control entity.

2000: Two Netscreen co-founders prematurely depart NetScreen to found Fortinet, a direct competitor to NetScreen, yet maintain equal ownership of NetScreen. Once again, the founders receive significant private financing despite the growing number of high-end industry competitors such as Cisco and Checkpoint.

2001: Successful IPO in months following 9/11 when the majority of IPO's were cancelled and IT and IT security related sales plummeted due frozen CAPX budgets during this period. NetScreen's financials included a significant number of anomalies associate with potential sales fraud executed from 1997 to their acquisition by Juniper in 2004.

2002: During the post IPO and pre Juniper acquisition period, Juniper was able to close the duress acquisition of OneSecure. OneSecure, an Israeli affiliated company with links to market leading Checkpoint, provided NetScreen with technical credibility required to increase sales within the U.S.

2003: The surprise duress acquisition of Neoteris in October 2003. Neoteris was a leading niche SSL/VPN company and the objective and value of this acquisition is not clear. Neoteris had an anomalous senior technical employee, another child of the Chinese Cultural Revolution, and a late 1980's Nanjing University Graduate. He was listed as a co-inventor of the SSL/VPN technology yet his education and career, till Neoteris, provided little access to the knowledge and experience one would normally associated with encryption technology development.

2004: NetScreen was acquired by Juniper for $4.1B. This valuation was based on an extremely high compound quarterly growth rates ranging from 14% to 80% during the preceding year. Its competitors

such as Nortel, Nokia, Checkpoint and SonicWall were averaging negative growth rates during the same period. NetScreen's success was reportedly based on major deals provided by the Government of China through it key SOE's – including a portion of the Great China Firewall.

2004-2006: 1) NetScreen became Juniper's primary security product's business unit, 2) NetScreen's founding executives led efforts to move NetScreen R&D to China, 3) Juniper's CEO signed a strategic partnership with Tsinghua University, 4) NetScreen's founding executives co-founded Northern Light Ventures (a high risk China/US venture firm), 5) a segment of NetScreen/Juniper leaders and employees founded Palo Alto (a competitor to Juniper), 6) a segment of NetScreen/Juniper leaders founded Sigma-RT (funded by Northern Light), 7) a segment of NetScreen/Juniper leaders founded Hillstone Networks (funded by Northern Light), 8) a key NetScreen founder became President of HYSTA (command and control entity), and 9) the same key NetScreen founder became co-chairman of Tsinghua Executive Entrepreneur Club (TEEC) in Silicon Valley.

2008: NetScreen/Juniper engineers adopt an encryption model for their SSL/VPN solution known to be susceptible to hacking and implement it in a manner that further weakens it.

2009: A key NetScreen founder is selected for membership in the China Entrepreneur Club – the most significant and elite, China Government led, cyber-economic command and control entity. Fortinet experiences 19% growth during the 2008-2009 global economic crisis.

2012-2013: 1) Key NetScreen and Fortinet founder becomes President of HYSTA, 2) ScreenOS Encryption Backdoor embed occurs and 3) ScreenOS Privileged Access Backdoor embed occurs

2014: 1) Juniper awarded unusual level of contracts within China despite the "Snowden-Effect" impact on peer U.S. competitors, 2) Juniper CEO mysteriously fired due to conduct in customer negotiation (some references to "intrigue"), and 3) Fortinet and Palo Alto leap over Juniper to take the #3 and #4 market positions respectively – while China-based, Northern Light Venture funded, Hillstone Networks experiences market leading growth rates despite a mature market

2015: Juniper releases an announcement regarding the recent detection of unauthorized code embedded within the Juniper ScreenOS that enabled two covert backdoors – one of which provided full administrative access while the other provided the ability to decrypt VPN connections. These backdoors provided the responsible threat with fully covert and unencrypted access to the encrypted traffic transmitted through a large number of internet service providers used by millions of private and commercial customers – including the DC, New York and Chicago regions. The system-development-lifecycle for ScreenOS has been controlled by Chinese employees from 1997 to the time of this incident. The quality assurance process may have been led by former Netscreen employees working for Sigma-RT – a Northern Light Venture company.

The IT Security campaign has expanded well beyond the entities noted above. And, the challenges of decoupling the legitimate entities and activities from the illegitimate becomes more and more difficult each month.

<u>Microchip Segment Campaign Highlights (2001-Current):</u>

The Microchip Segment Campaign is an example of a more sophisticated cyber-economic campaign that appears to be leveraging all the benefits of the historical IT industry campaigns as well as the lessons-learned. **This is China's current #1 priority campaign.**

This campaign, more so than any other technology segment, appears to involve a material level of support and coordination between Chinese operating from China's Mainland, Taiwan, U.S. and Europe. China has boldly communicated their objectives and provided a significant level of detail about their plans and involved entities.

This campaign is divided into sub-campaigns targeting the various categories of microchip technology. This includes microprocessors, chipsets, memory, CMOS, analog and power, mixed signal etc. This campaign appears to include an industry unique objective that, if understood by U.S. oversight organizations such as CFIUS, may help shed light on the risk of certain Chinese led investments and acquisition efforts that would otherwise appear low risk. China appears to be executing a cyber-economic campaign strategy designed not only to gain market leadership for its national champions but capture as much IC industry "capacity" as possible. Capacity refers to each competitor's share of the industry's manufacturing facilities, suppliers and raw materials. Some experts have indicated that there's only so much capacity available and this is why we'll often see market leading IC industry competitors acquire failing competitors that provide no obvious financial value.

This past August, China announced the formation of The "High End Chip Alliance (HECA)." This alliance would be considered an anti-trust cartel if it were within U.S. borders. The government's industry spokesperson from TrendForce stated "This alliance of government, academia (government), and industry aims to create a complete ecosystem for domestic semiconductor manufacturers. If successful, the alliance will create a chip industry chain starting from chip architecture to chip production, operation systems, devices, platforms and finally to the IT service market." And then, Jian-Hong Lin stated "The mission of China's high-end chip alliance is to develop highly localized and vertically integrated relationships among industry players. The ecosystem they built will be exclusively for domestic manufacturers and design houses." This exclusive cartel consists of 27 members – including Tsinghua Unigroup, SMIC, Yangtze River Storage Technology, Lenovo, ZTE, Beijing University, Tsinghua University, Chinese Academy of Sciences, Baidu and Alibaba. The Director of this Cartel will be Ding Wenwu, President of China's National Semiconductor Industry Investment Fund. The Deputy Cartel Director is Tsinghua Unigroup Chairman Zhao Weiguo. These are two Chinese government representatives.

This industry segment campaign relies heavily on the following methods/tactics:

1. "Power Buyer" coercion and leverage gained as a result of the market share and leadership positions gained as a result of their IT Industry Campaign within rare earth materials (90%), telecom, enterprise communications, mobile, PC, servers and the Internet of Things (especially automotive)
2. Aggressive investments in, or acquisitions of, industry capacity
3. Aggressive "cross-straits" (Taiwan) recruiting, infiltration, investments and acquisitions
4. Embedded insider threat actors working within all the western microchip manufacturers and investment entities
5. NDRC assisted duress on western competitors operating within China
6. Additional leverage gained as the result of HNA Group's acquisition of Ingram Micro

<u>Media & Entertainment Segment Campaign Highlights:</u>

The Media and Entertainment Segment Campaign substantially overlaps with the IT Industry Campaign. As with other strategic campaigns substantially launched after President Xi assumed leadership of ChinaCo, an industry reference used to capture the notion a Chinese National Conglomerate consisting of all commercial entities, this is a more sophisticated cyber-economic campaign than those launched in the late 1990's. It too appears to be leveraging all the benefits of the historical IT industry campaigns as well as the lessons-learned. This campaign also appears to have much great significance to China than most policy makers understand due it's links to the Ministry of Propaganda initiatives. This segment campaign includes:

1. Mobile and online games
2. Internet browsers
3. Media content (archived movies, television shows, online distribution services etc.)
4. Data streaming and content delivery
5. Automatic Content Recognition (ACR)
6. Production studios
7. Resorts and Theme Parks
8. Cruise lines
9. Sports and Sport Media

The cyber-economic methods and schemes associated with this campaign mirror those noted earlier. The most significant beneficiaries and investors associated with this campaign include: 1) Wanda Group, 2) Alibaba (YF Capital, Alibaba Digital Media and Entertainment, and Alibaba Pictures), 3) Tencent, 4) Tang Media Partners, 5) China Media Capital, 6) Huayi Brothers, 7) Fosun Capital, 8) CITIC, 9) Flagship Entertainment, 10) Shanghai Giant Network Technology, 11) Hunan Television & Broadcast 12) Leyou Technologies, 13) Shandong Hongda, 14) LeVision, 15) LeEco/Vizio, 16) PCCW Media and 17) Crunchyroll

The large number of elite Chinese Government controlled investors is a clear indicator of the importance and priority associated with this campaign.

<u>Financial Industry (FinTech)</u>

The Financial Industry (FinTech) Segment Campaign substantially overlaps with the IT and Media and Entertainment Industry Campaigns. It too represents a more sophisticated campaign. As with the microchip segment campaign, if the current cyber-economic risk scenarios associated with this campaign come to fruition, the impact on the U.S. economy and national security are quite severe.

To understand the quality of the banking and financial services industry campaign strategy, we must view the strategy within the context of the last four campaigns described to this commission as well as the insurance industry segment campaign. "ChinaCo" increasingly controls the servers, laptops and mobile devices and software we use to manage our financial processes, play online games, watch online news, movies and television shows, secure our mobile devices and secure our browsers.

The current U.S. financial services and asset management industry leaders are incredibly strong but also incredibly vulnerable to unexpected changes driven by emerging and disruptive technologies. ChinaCo's

cyber-economic campaign strategy for this industry appears to be based on a four-prong attack. Each prong (CE risk scenario) is described below and our assessment is based on the evidence collected over the past four months:

1. **Industry Infiltration & Degradation**: Traditional investment, joint-venture and insider infiltration strategy supported by unique Chinese resource management organizations such as UniCareer
2. **FinTech Vertical Monopoly**: Alibaba, Tencent, Baidu, Ping An, JD.com and Xiaomi have launched FinTech capabilities in nearly all vertical FinTech categories. This would typically be considered a vertical monopoly and anti-trust violation.
3. **FinTech Horizontal Monopoly:** Huawei, Lenovo and Xiaomi have launched major FinTech infrastructure solutions designed in a manner consistent with a horizontal monopoly structure. When coupled with the advantages gained as a result of the vertical monopoly, ChinaCo gains an incredible amount of industry advantages and an ability to block all competitors from challenging its FinTech position.
4. **Digital Transaction Monopoly:** ChinaCo appears to be executing an aggressive IP theft and conversion campaign, as well as state-sponsored acquisition strategy to corner the bitcoin and blockchain market and introduce the first major disruptive innovation in the financial transaction and asset management industry in recent memory. This technology is already being integrated with some of Chinese FinTech vertical and horizontal solutions. Successful execution of this strategy will undermine all current leaders in the industry. Key high risk entities associated with this campaign include all organizations subordinate to Financial Blockchain Shenzchen Consortium (FBSC) and the Chinese representatives to the R3 Blockchain Consortium. The Zhongguancun Science Park and the following universities are key to China-based R&D and conversion activities: 1) Tsinghua University, 2) Peking University, 3) CAS/CAE, 4) Renmin University and 5) Beihang University.

Which Chinese, or Chinese Controlled, Investors present the highest risk to U.S. interest?
Our efforts indicate the following investors are the highest risk to U.S. national interest: 1) Alibaba syndicate, 2) Wanda Group syndicate, 3) Tsinghua syndicate, 4) Fosun syndicate, 5) Tencent syndicate, 6) Legend syndicate, 7) Huawei syndicate, 8) CITIC syndicate, 9) Northern Light Ventures syndicate, 10) Summitview syndicate, 11) Shanghai Semiconductor syndicate, 11) China Integrated Circuit Industry Investment Fund (CICIF) syndicate.

In addition, I believe special attention should be paid to: 1) China Entrepreneur Club, 2) HYSTA and U.S. based investors and companies with close relationships with the investor syndicates and suspected command-and-control entities described above.

What other activities have the Chinese been involved in that might advance their interests to the disadvantage of U.S. companies?
China's most effective means of gaining tactical and strategic advantage over U.S. companies is something most American's are just not prepared to listen to or address. But, it is also the method that could be the Achilles Heel of the entire Chinese cyber-economic campaign strategy.

The method used is so detestable to our personal sensitivities that it is just as controversial to speak of it as it is to speak about the differences between torture and acceptable forms of interrogation.

The method I am referring to is the use of a massive human intelligence, open-source intelligence and technology transfer networks to infiltrate and exploit foreign competitors, R&D organizations and universities for the purposes of IP theft, espionage, sabotage and capacity building.

Considering the stated goals and objectives of the United Front and Overseas Chinese Affairs Office, it appears likely China intends to leverage as many overseas Chinese, and persons of Chinese descent, as possible in order to achieve their long-term national objectives. The advantage this provides far exceeds that of traditional, externally focused, cyber access. It provides trusted insider access as well as control and influence within the targeted competitors.

According to the U.S. Census Bureau, as of 2013, 2,018,000 Chinese immigrants lived within the U.S. 1,634,000 of these immigrated to the U.S. after 1980 and most were raised within the Communist led academic, legal and social environment while a small percentage were raised in Hong Kong. In addition, according to the Wall Street Journal, in 2015, there were 331,371 Chinese students studying within the U.S. – more than double that from India. Conversely, the number of Americans living on the Chinese mainland reached a mere 71,493 in 2010 – many of which are of Chinese discent (Chinese census bureau figures). As noted within Chinese sourced policy documents, much of the Ministry of Science & Technology, Ministry of Personnel, Chinese Academy of Sciences, Ministry of Education, National Natural Science Foundation (NSFC), State Administration of Foreign Expert Affairs (SAFEA), Overseas Chinese Affairs Office and United Front efforts are focused on optimizing the impact of these overseas Chinese as well as optimizing the Chinese Returnee contributions upon return to the mainland.

Another unique advantage Chinese corporations and investors have over their U.S. counterparts is their apparent immunity to Foreign Corrupt Practices Act (FCPA) restrictions. Corporate leaders are able to make “major investments” in opportunities with little or no expectation of receiving a traditional ROI because the cost lines within their budgets mean little when the government provides covert subsidies, loans, grants and even debt relief. This allows any number of Chinese corporate leaders to invest in deals that benefit U.S. political leaders, their families or allies in anticipation of a quid-pro-quo on future policies impacting China or Chinese investments. Two such anomalous investments involved Shandong Tranlin Paper Co. Ltd (aka Quanlin Paper) and Shandong Sun Paper Industry Co. Headlines indicated these investments were to be at the $2B and $1.36B level and for the purposes of establishing pulp plants in the Virginia and Arkansas. Neither investment appears to conform with traditional ranges for such investments, Virginia and Arkansas are not in the top tier for straw production required to support operations, and the U.S. pulp market is experiencing a negative annual rate. These investments may have been attempts to influence the U.S. political process as the U.S.

Another unique advantage provided to China’s industry leaders comes from China’s unique use of a small number of key billionaires that appear to act as a direct agent or conduit to and from President Xi. Two of the most noteworthy noted within the SquirrelWerkz case studies include Jack Ma (Alibaba) and Jianlin Wang (Wanda). Considering the campaigns led by these two individuals, it would be difficult to identify two more significant Chinese threats to U.S. economic and national security interests than these two individuals.

Finally, China's National Development and Reform Commission (NDRC) has introduced yet another material advantage to China's industry players. The NDRC now appears to play an active role in applying strategic duress on foreign competitors that extends well beyond normal regulatory and enforcement support. In addition, it's unique role in investigating foreign companies for perceived anti-trust violations provides yet another mechanism for accessing and sharing sensitive IP seized during these same investigations.

Are there concerns that Chinese government-affiliated entities, through private equity investments, may gain access to U.S. companies that produce advanced materials or technologies that have dual-use applications?

Example #1: Undersea Cable Industry

Evidence supports a conclusion that China poses a significant threat to the U.S. Navy and its allies due its long-term efforts to gain incremental control of the foreign companies associated with the undersea cable industry and the potential enhancement of these cables to support undersea monitoring and command and control. Despite direct control of less than 10% of the current total market through Huawei Marine, China has gained considerable control/influence over the top providers including: 1) Nokia's Alcatel-Lucent Submarine Networks (ASN) Division, 2) TE Connectivity Inc/SubCom and 3) NEC.

Example #2: Navy Shipbuilding Industry

Evidence supports a conclusion that China is leveraging its cyber-economic methods and entities to access classified and sensitive engineering documents, plans and specifications. Chinese shipbuilders such as CSIC, CSSC, CSTC and SinoTrans/CSC appear to be leveraging ChinaCo's broader campaign relationships, access and leverage points to gain access to these types of documents, technology and the skilled resources through companies based within allied nations such as Taiwan, France, Turkey, Germany, Pakistan, Saudi Arabia, Egypt, UAE and India. In addition to the aforementioned Chinese shipbuilders, the following Top 5 Chinese entities appear to be involved in the conversion efforts: 1) Harbin Institute of Technology, 2) Harbin Engineering University, 3 Beijing Institute of Technology, 4) University of Science and Technology of China and 5) Beihang University).

One Navy related example includes the apparent use of sales related incentives and dis-incentives to manipulate Rolls-Royce to, wittingly or unwittingly, provide access to sensitive propulsion-related engineering IP. In excess of 10% of Rolls-Royce revenue comes from China and Rolls-Royce is also a major provider of advanced propulsion systems for the U.S. Navy. The PLAN has improved its own submarine fleet's propulsion systems using IP provided through Rolls-Royce. In addition, China has sold no less than two attack submarines and two destroyers to Pakistan with the same advanced propulsion systems.

Other concerning defense related cyber-economic campaign indicators are associated with the following: 1) autonomous vehicles (automobiles, trucks, aircraft, shipping and submersibles,), 2) drones, 3) advanced rocket propulsion systems, 4) private space industry, 5) virtual reality, 6) aerospace and aerospace supply-chain.

Key Space Industry Activities and Entities:

1. China's OneSpace was founded in June of 2015 with direct support from the National Defense Science and Industry Bureau and is the Chinese competitor of U.S. based SpaceX. Its core investors include Legend Holdings (Lenovo), Harbin Institute of Technology (HIT), Chun Xiao Capital and Land Stone Capital
2. Other emerging space industry entities include Landspace (Tsinghua), Shenzhen Yu Long Aerospace Science and Technology, Expace, Link Space, Space Vision and Blue Origin
3. The China Academy of Launch Vehicle Technologies (CALT) leads China's public and private sector investments and development associated with spaceplanes
4. The KuancgChi Group syndicate is highly involved in space related investments including a $1.5B futuristic tourism and space theme park. Kuang-Chi is China's answer to Elon Musk and his organization already ranks #7 in patent applications
5. AVIC acquired California based Align Aerospace in 2015. Align is a global aerospace supply chain company providing a wide variety of proprietary and non-proprietary products and hardware required for aircraft manufacturing and maintenance. This acquisition provides AVIC direct buyer and technology partner access to GE, Pratt, Bell, Sikorsky, Honeywell, Triumph, Boing and Bombardier.

What do public and private sector policy leaders need to understand to gain a greater appreciation of the threat to U.S. interest caused by China's outbound investment strategy?

During the past four years, I've met privately with more than 300 senior executives representing more than 20 industries. During these meetings, we've either reviewed the China led cyber-economic campaign having to do with their company or industry. In nearly every case, the executives have agreed with, and often validated, the findings and evidence. And, in nearly every case, these same executives provide their own examples of incidents and indicators and express a desire to take action. But, there are two consistent mental obstacles that tend to prevent or minimize their response:

1. They have no meaningful reference point to help them understand how big, complex, effective and persistent the Chinese Cyber-Economic Threat really is so they begin to believe they can just hunker down and the storm will pass
2. They are fearful that if they take meaningful action, the Chinese threat actors will take revenge in ways that destroy their business, reputation and ability to recover

Addressing the first issue could be accomplished through a government led effort to educate the public and private sector on the true nature of the two primary nation-state cyber-economic threats (China and Russia). This education process should include U.S. universities and research organizations and include a review of the following:

China's Economic and S&T Intelligence Requirements, Collection and Conversion Process consist of six stages: 1) Communist Party Defines/Documents Key Themes, Main Task and Strategic Priorities for S&T/Economic Growth, 2) Consumers of S&T/Economic Intelligence Define Requirements to satisfy Communist Party objectives, 3) S&T/Economic intelligence collection managers task collection resources, 4) S&T/Economic intelligence collection resources collect and transfer raw intelligence to analysis and processing resources, 5) S&T/Economic intelligence analysis and processing resources

prepare information for use and distribution to consumers and 6) S&T/Economic intelligence consumers further sanitize and convert IP into economic advantage.

Communist Party Defines/Documents Key Themes, Main Task and Strategic Priorities for S&T/Economic Growth*:*

1. All S&T/Economic goals, objectives and budget approvals are defined within the context of China's Five Year Plans (FYPs)
2. The State Council, the most powerful decision authority in China, is led by the President/Premier and includes 32 ministry leaders
3. State Council Departments support &/or assists in the development of the specific industry/product segment plans and budgets
4. National Development and Reform Commission (NDRC) is the most influential FYP leadership organization
5. NDRC has recently assumed an additional role that includes an authority to levy anti-trust claims and penalties against corporations for activity, which is currently or historically has been authorized – This provides the NDRC with a powerful economic weapon

Consumers of S&T/Economic Intelligence Define Requirements to satisfy Communist Party objectives.

1. The State Council Steering Committee of S&T and Education Coordinates the National S&T Policy (including the National Innovation System Policy)
2. The State Council Steering Committee of S&T and Education members represent the top five national S&T planning, intelligence process management, conversion and capacity building organizations/programs
    - Ministry of Science & Technology (MOST)
    - Chinese Academy of Sciences (CAS)
    - Ministry of Education (MOE)
    - Ministry of Personnel (MOP)
    - National Natural Sciences Foundation
3. The military S&T/Economic information governing body interacts directly with the President and State Council to ensure the highest priorities are assigned to their requirements

S&T/Economic intelligence collection managers task collection resources. There are three primary categories of S&T/Economic Intelligence Collection Managers:

1. PLA (Military Intelligence)
2. Ministry of State Security (Foreign Intelligence Service)
3. Civilian (Economic and Corporate Espionage)

The PLA has four primary units tasked with the collection and exploitation of Foreign S&T/Economic Intelligence. The MSS has three primary units tasked with the collection and exploitation of Foreign S&T/Economic Intelligence. There are no less than eight civilian ministries or departments tasked with the collection and exploitation of Foreign Economic and S&T Intelligence. Each of the three primary intelligence managers relies heavily upon overseas Chinese and their "insider" status to accelerate and optimize S&T/Economic Intelligence collection, analysis, storage and transmission to the processing and storage resources.

S&T and Economic Ministries plan, fund and support the S&T and economic intelligence exploitation and processing requirements – including the human resources and capacity building efforts.

The Ministry of Science & Technology (MOST) acts as the overall "Project Manager" for the collection, whitewashing, and conversion of Foreign S&T/Economic Intelligence through:

1. National S&T Programs
2. State Key Laboratories
3. National Engineering Research Centers
4. High-Tech Development Zones

The **Chinese Academy of Sciences (CAS)** acts as the single most significant R&D, white paper and patent conversion entity. The **Ministry of Personnel** acts as the primary organization for short and long-term capacity building, recruiting talent for domestic and overseas positions, motivating overseas Chinese to support the motherland and ultimately return to the mainland. The **Ministry of Education** serves to prepare specific individuals for overseas assignments, manage international exchange programs, manage intelligence storage/database operations and support the whitewashing and conversion processes. The **National Natural Science Foundation (NSFC)** serves a critical role between the ministries, academic environment and industry by funding and providing oversight for strategic research efforts and institutions.

Chinese source documents indicate that as of 2005, China funded and operated no less than 353 major S&T and economic intelligence institutes nationwide. This infrastructure and resources should be considered an illegal subsidy and a significant component of the criminal cartel involved in cyber-economic campaign activity. These brake down into:

- ~35 attached to the technical ministries
- ~33 subordinate to provincial and municipal governments
- ~285 considered local institutes
- ~15,782 direct employees

In addition to this, there are ~3,000 basic cells serving in key requirements generation and conversion positions. Chinese source documents refer to approximately 60,000 employees in grassroots units such as "companies" and "labs." These resources are assigned duties defined as "investigating, collecting, sifting, analyzing, synthesizing and repackaging data in response to specific requirements." SquirrelWerkz assumes, based on its own evidence, these resources serve within the intelligence liaison and management role within key Chinese companies (e.g., National Champions) and assist with the conversion of stolen IP and open-source intelligence into competitive advantage and competing products for these companies.

S&T and Economic Intelligence Collection Resources collect and transfer raw intelligence to analysis and processing resources through a wide variety of transfer methods – both overt and covert.

- Overt: Performed with little effort to conceal the actual collection activities

- Covert: Performed within a clandestine environment with the intent of concealing the collection activity or the true-nature of the collection activity

The China-PRC National Innovation System and "Information/Intelligence" Processing and Dissemination Programs follow the former Soviet Model for planning and collection but have been enhanced to incorporate the strengths and cultural nuances of China

- Layered approach to intelligence collection (Mattis) ranging from traditional service-driven operations with modern tradecraft to "amateur espionage" entrepreneurs
- Maximize numbers of "agents" or resources instead of a smaller, trusted, cadre of collectors
- Train the millions of "amateur agents" or resources to focus on denial versus tradecraft – get lost in sheer volume

Chinese and U.S. source documents indicate the Chinese government goals and objectives include a desire to control and manage all Chinese – including mainlanders, overseas, and even those with no direct family ties – through active insertion into foreign communities, associations, and control of local community organizations (Tongs) and Triads.

Economic and S&T Analysis and Processing Resources prepare Information for use and distribution to consumers.

China's National S&T/Economic Civilian Intelligence (Information) Governing Body includes three key and inter-related entities:

1. Ministry of Industry Information & Technology (MIIT)
2. State Administration of Science, Technology and Industry for National Defense (SASTIND)
3. Civil Military Integration Promotion Department (CMIPD)

China's National Economic and S&T Civilian Intelligence (Information) Governing Body includes seven subordinate member organizations. There are reportedly three National S&T/Economic Intelligence Analysis & Processing Organizations (mega-libraries):

1. China Defense Science & Technology Information Center (CDSTIC)
2. National Science & Technology Library (NSTL)
3. Patent Documentation Library

There are no less than thirteen subordinate S&T and National Economic Intelligence Analysis & Processing Organizations.

PLA source documents indicate there are three primary differences between these Libraries and western notions of libraries: 1) the Chinese system is run by intelligence experts, 2) they directly and actively support end-users and 3) they have a mission to provide an R&D shortcut by leveraging foreign intelligence

Other source documents indicate that in 2005, there were 50,534 networks used to host and distribute S&T information, 27,000,000 users and 1,000,000+ Chinese accessing “overseas” networks through the Intelligence Institutes to gather foreign S&T materials.

S&T/Economic Intelligence Consumers (aka, cyber-economic campaign beneficiaries) further sanitize and convert stolen confidential information and intellectual property into economic, competitive and military advantage.

Chinese source documents indicate there are three primary conversion environments used to transform (re-innovate) the S&T and economic Intelligence into usable forms that provide Chinese entities with an economic advantage (indigenous innovation).

1. Academic: Used to whitewash the stolen or improperly attributed IP and to gain international competitive advantage for purposes of increasing tuition revenues, patent royalty revenues, entice foreign student registration, entice overseas Chinese to return and attract otherwise undeserved Inward-Forward Direct Investment (I-FDI) related to ongoing research and development efforts (illicit subsidies)
2. Commercial: Used to produce competitive products and gain industry advantage without the corresponding cost-of-goods, R&D or capital expenditures (illicit subsidies)
3. Military: Used to produce competitive aerospace and defense systems and strategic advantage as well as to counter foreign systems and advantages

China’s National Innovation System (NIS) and Economic and S&T Intelligence Network is massive in size and scope, yet is managed in a highly effective manner due to the investments made to shape and control the collectors and conversion process within the context of China’s broader, long-standing, institutional, academic, research and economic development structures.